Amendments to the Claims

1. (previously presented) A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a right portion of an input bit sequence for the current cryptographic round;

first circuitry configured to perform an exclusive OR (XOR) on the expanded first bit sequence and a key provided by the key scheduler to generate a third bit sequence;

a substitution box (SBox) configured to transform the third bit sequence into a fourth bit sequence;

second circuitry configured to perform an exclusive OR (XOR) on the fourth bit sequence and a left portion of the input bit sequence for the current cryptographic round to generate a fifth bit sequence;

permutation logic coupled to the expansion logic and the second circuitry, the permutation logic configured to receive the fifth bit sequence from the second circuitry and to perform a permutation of the fifth bit sequence,

wherein the fifth bit sequence is a right portion of an output bit sequence of a current cryptographic round.

2.- 3. (canceled)

4. (previously presented) The cryptography engine of claim 1 further comprising two-level multiplexer circuitry, wherein a first level of the two-level multiplexer is configured to receive an inverse permutation of a first portion of the input bit sequence and an inverse permutation of a second portion of the input bit sequence during an initial cryptographic round and a right portion of an output bit sequence from a previous cryptographic round during a subsequent cryptographic round and wherein a second level of the two-level multiplexer is configured to receive the output of the first level and the right portion of the output bit sequence generated during the previous cryptographic round.

5. (original) The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. (original) The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7. (original) The cryptography engine of claim 5, wherein the expanded first bit sequence is less than 48 bits.

8. (original) The cryptography engine of claim 6, wherein the expanded first bit sequence is less than six bits.

9 – 12. (canceled)

13. (original) The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

14. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a plurality of stages.

15. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

16. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a shift stage.

17. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

18. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

19. (previously presented) The cryptography engine of claim 1, wherein a first shift amount for a first key is identified in a determination stage using a first round counter value.

20. (canceled)

21. (previously presented) The cryptography engine of claim 4, wherein the two-level multiplexer is configured to swap a left portion of the output bit sequence of a previous cryptographic round with a right portion of the output bit sequence of the previous cryptographic round, whereby the right portion of the input bit sequence of the previous cryptographic round becomes the left portion of an input bit sequence for the current cryptographic round and the fifth bit sequence becomes a right portion of the input bit sequence for the current cryptographic round.

22. (canceled)

23. (previously presented) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a right portion of an input bit sequence for the current cryptographic round;

first circuitry configured to perform an exclusive OR (XOR) on the expanded first bit sequence and a key provided by the key scheduler to generate a third bit sequence;

a substitution box (SBox) configured to transform the third bit sequence into a fourth bit sequence;

second circuitry configured to perform an exclusive OR (XOR) on the fourth bit sequence and a left portion of the input bit sequence for the current cryptographic round to generate a fifth bit sequence;

permutation logic coupled to the expansion logic and the second circuitry, the permutation logic configured to receive the fifth bit sequence from the second circuitry and to perform a permutation of the fifth bit sequence,

wherein the fifth bit sequence is a right portion of an output bit sequence of a current cryptographic round.

24. - 25. (canceled)

26. (previously presented) The integrated circuit layout of claim 23 further comprising two-level multiplexer circuitry, wherein a first level of the two-level multiplexer is configured to receive an inverse permutation of a first portion of the input bit sequence and an inverse permutation of a second portion of the input bit sequence during an initial cryptographic round and a right portion of an output bit sequence from a previous cryptographic round during a subsequent cryptographic round and wherein a second level of the two-level multiplexer is configured to receive the output of the first level and the right portion of the output bit sequence generated during the previous cryptographic round.

27. (previously presented) The integrated circuit layout of claim 23, wherein the first bit sequence is four bits.

28. (previously presented) The integrated circuit layout of claim 27, wherein the expanded first bit sequence is less than six bits.

29. (previously presented) The integrated circuit layout of claim 23, wherein the key scheduler performs pipelined key scheduling logic.

30. (previously presented) The integrated circuit layout of claim 23, wherein the key scheduler comprises a determination stage.

31. (previously presented) The integrated circuit layout of claim 23, wherein the key scheduler comprises a shift stage.

32. (previously presented) The integrated circuit layout of claim 23, wherein the key scheduler comprises a propagation stage.

33. (previously presented) The integrated circuit layout of claim 23, wherein the key scheduler comprises a consumption stage.

34. (previously presented) The integrated circuit layout of claim 23, wherein a first shift amount for a first key is identified in a determination stage using a first round counter value.

35. (canceled)

36. (previously presented) The integrated circuit layout of claim 26 , wherein the two-level multiplexer is configured to swap a left portion of the output bit sequence of a previous cryptographic round with a right portion of the output bit sequence of the previous cryptographic round, whereby the right portion of the input bit sequence of the previous cryptographic round becomes the left portion of an input bit sequence for the current cryptographic round and the fifth bit sequence becomes a right portion of the input bit sequence for the current cryptographic round.

37. (canceled)

38. (previously presented) The cryptography engine of claim 1, wherein the first circuitry comprises:

a plurality of logic devices simulating an XOR operation for combining the key provided by the key scheduler with the expanded first bit sequence, the plurality of logic

devices including a multiplexer receiving first and second input values and an OR logic combining an output value of the multiplexer with a third input value;

wherein the first, second, and third input values are determined based on the key provided by the key scheduler and further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations.

39 -40. (canceled)

41. (previously presented) The cryptographic engine of claim 4, wherein the first level comprises:

a first two to one multiplexer, and

a second two to one multiplexer; and

wherein the second level includes:

a third two to one multiplexer coupled to the first two to one multiplexer, and

a fourth two to one multiplexer coupled to the second two to one multiplexer.

42. (previously presented) The cryptographic engine of claim 1, wherein the expansion logic comprises:

a first expansion logic block coupled to the first circuitry and configured to receive the first bit sequence; and

a second expansion logic block coupled to the second circuitry and to the first circuitry configured to receive the fifth bit sequence from the second circuitry.

43. (previously presented) The cryptographic engine of claim 1, further comprising:

a first asynchronous FIFO configured to convert input blocks of a third size to blocks of a fourth size for cryptographic processing; and

a second asynchronous FIFO configured to convert cryptographic output blocks of the fourth size to the third size for further processing.

44. (canceled)